PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-339273
(43)Date of publication of application : 08.12.2000

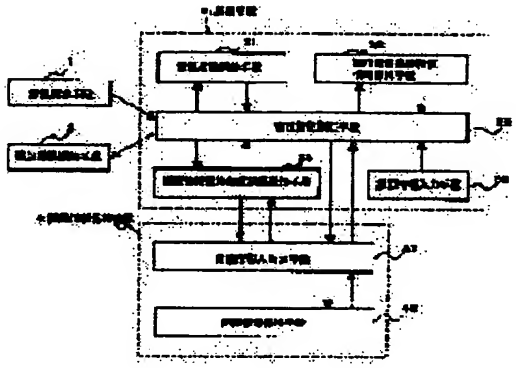
(51)Int.Cl. G06F 15/00

(21)Application number : 11-152382
(22)Date of filing : 31.05.1999

(71)Applicant : NEC CORP
NEC SOFTWARE TOHOKU LTD
(72)Inventor : KOMATSU FUMIKO
HIDANO MORIMITSU

(54) INFORMATION PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a device which simplifies an authentication procedure at the time of using an application and, at the same time, enables authentication information to be used in common by plural applications.
SOLUTION: This device is an authentication system which enables authentication information for a user to be used in common among plural applications for performing authentication when the user accesses the information. When the system is fitted with an authentication information holding device 4 which is freely attachable/detachable and stores the authentication information, in active state and authentication is already performed, an authentication procedure at the time of using the application is not performed but the application is accessed as it is. When the authentication information holding device 4 is removed and is not activated, switch control is performed so that an authentication procedures needed by the application is performed in using the application.



LEGAL STATUS

[Date of request for examination] 21.04.2000
[Date of sending the examiner's decision of rejection] 12.08.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－339273
（P2000－339273A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ　５Ｂ０８５

審査請求　有　　請求項の数８　ＯＬ　（全　９　頁）

(21)出願番号　特願平11－152382

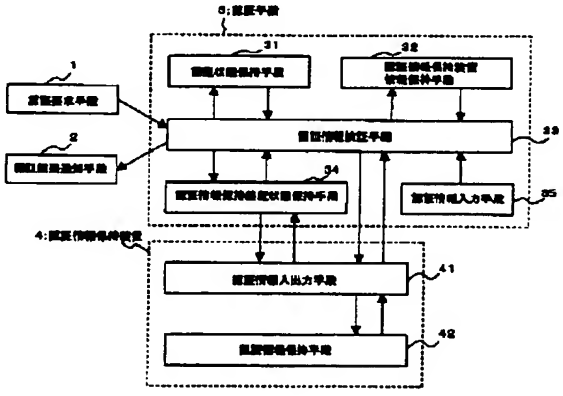
(22)出願日　平成11年５月31日(1999.5.31)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(71)出願人　000222059
東北日本電気ソフトウェア株式会社
宮城県仙台市青葉区一番町一丁目10番23号
(72)発明者　小松　文子
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100080816
弁理士　加藤　朝道

最終頁に続く

(54)【発明の名称】　情報処理装置

(57)【要約】
【課題】アプリケーション利用時の認証手順を簡素化するとともに、複数のアプリケーションで認証情報を共用可能とする装置の提供。
【解決手段】ユーザがアクセスする際に認証を行う複数のアプリケーション間で前記ユーザの認証情報を共有可能とする認証システムであって、認証情報を格納する着脱自在な認証情報保持装置が装着されて活性化状態にあり、且つ、認証済みである場合には、アプリケーションの利用時の認証手続は行わず、そのまま前記アプリケーションがアクセスされ、一方、前記認証情報保持装置が外されている等活性化されない時には、アプリケーションを利用する際に前記アプリケーションで必要とされる認証手続を行うように切替制御する。



1

【特許請求の範囲】

【請求項１】ユーザがアクセスする際に本人認証を行う複数のアプリケーション間で前記ユーザの認証情報を共有可能とする情報処理装置であって、

認証情報を格納する着脱自在な認証情報保持装置が装着されて活性化状態にあり、且つ、認証済みであることを検出した場合には、アプリケーションの利用時の本人認証手続きは行わず、そのまま前記アプリケーションがアクセスされ、一方、前記認証情報保持装置が活性化できない時には、アプリケーションを利用する際に前記アプリケーションで必要とされる本人認証手続きを行うように切替制御する手段を備えたことを特徴とする情報処理装置。

【請求項２】前記着脱自在な認証情報保持装置記が、ユーザからの本人認証情報を入力する手段と、認証情報の検証を行なう手段と、認証情報を保持する手段とを含むことをことを特徴とする請求項１記載の情報処理装置。

【請求項３】認証情報を着脱自在な認証情報保持装置に記憶保持し、

アプリケーション利用の際の本人認証時、認証要求を受けた際に、前記認証情報保持装置が装着されて活性化状態とされ、且つ記憶手段に保持された、認証済みであるか否かを示す認証状態情報が認証済みであることを示す場合には、認証手順を省略して認証成功を通知するように制御する手段を備え、前記アプリケーションは認証成功の場合、本人認証手続きを省略し、

前記認証情報保持装置が活性化状態にない場合、もしくは活性化できない場合、前記認証状態情報をリセットし、前記アプリケーションで必要とされる本人認証手続きを行なうように制御する手段を備えたことを特徴とする情報処理装置。

【請求項４】アプリケーション利用の際の本人認証時、前記認証情報保持装置が装着状態にあり、前記認証状態フラグが認証済みでないことを示す場合には、本人認証手続きを実行し、本人であることが認証された場合、前記認証状態情報を認証済みに設定する手段を備えたことを特徴とする請求項３記載の情報処理装置。

【請求項５】前記着脱自在の認証情報保持装置の装置の特性及び状態を取得する手段を備えたことを特徴とする請求項３記載の情報処理装置。

【請求項６】アプリケーションで本人認証手続きが必要とされた場合に前記アプリケーションから起動される認証要求手段と、前記認証要求手段からの認証要求を受け取り、着脱自在の認証情報保持装置の状態情報を取得し、活性化状態であれば、認証状態を取得し、未認証状態であれば、前記認証保持装置が保持しているユーザ本人の認証情報と、入力手段から入力された認証情報との照合を行い、ユーザ本人であることを認証がなされた場合、認証状態を認証済みに設定し、認証済み状態であれば、認証処理を省略し認証成功を認証結果通知手段に出力する認証手段を備え、前記認証成功が出力された場合、前記アプリケーションは本人認証手続きを省略する、ことを特徴とする情報処理装置。

2

【請求項７】前記認証情報保持装置が、記憶媒体もしくはＩＣカードよりなることを特徴とする請求項３乃至６のいずれか一に記載の情報処理装置。

【請求項８】前記アプリケーションは、前記認証要求手段と前記認証結果通知手段を介して前記認証手段と交信し、前記認証情報保持装置の制御は前記認証手段で行うことを特徴とする請求項６記載の情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置に関し、特に、情報処理装置で稼働するアプリケーションを利用する際の認証を行うシステムに関する。

【０００２】

【従来の技術】コンピュータ等情報処理装置上でアプリケーションを利用する場合、正当な利用者であることの認証を行うため、アプリケーションは、ログイン時、ユーザにユーザＩＤ及びパスワードの入力を督促し、入力されたユーザＩＤ、パスワードが登録されたものと一致する場合、アプリケーションの利用が許可される構成とされている。

【０００３】ところで、アプリケーションを利用するたびに認証手順を行うことは、煩雑であることから、ひとたび、本人から入力され照合された認証情報を、ハードディスクやメモリ上に保持し、２回目以降の本人認証には、該媒体に保持された情報を使用することで、認証回数を削減するようにしたアプリケーションも存在している。

【０００４】

【発明が解決しようとする課題】しかしながら、このように認証回数を削減する従来のシステムは、次のような問題点を有している。

【０００５】第１の問題点は、認証情報の漏洩など、セキュリティの面が十分に考慮されていない、ということである。

【０００６】その理由は、将来のシステムは、本人から入力された認証情報を、情報処理装置に固定のハードディスクやメモリ上に保持し、２回目以降の本人認証には、保持した情報を使用するというものであるためである。また、情報そのものが盗まれなくとも、例えば利用者が席を外している間に第３者が利用者になりすまし、不正にアプリケーションを利用することも可能である。

【０００７】第２の問題点は、情報処理装置で稼動するアプリケーションの数だけ本人認証が発生する、ということである。

【０００８】その理由は、アプリケーションによって実装方法が異なるため、アプリケーション間で認証情報を共有することができないためである。

3

【０００９】なおキーデータが電源供給中保持されることをなくすＩＣカードとして、特開平５－２５０５６２号公報には、外部からある命令を入力することで、認証情報の照合結果を内部的にクリアする手段を備え、認証情報の照合結果が電源供給中に保持されることがなくなり、途中で介在する不当者による不正アクセスを防止するようにした構成が開示されている。また特開平１０－２８５１５３号公報等には、利用者が自己のキーファイルを格納したＩＣカードを装着した場合、利用者認証が行われ、キーファイルをメモリに展開し、またＩＣカードが抜かれた場合、メモリからキーファイルを削除し、第三者への漏洩を防ぐ通信システムが開示されているが、これは、仮想専用回線利用時すなわち単一アプリケーション利用時のキーファイルの漏洩を回避するためのものである。

【００１０】したがって本発明は、上記問題点に鑑みてなされたものであって、その主たる目的はアプリケーション利用時の認証手順を簡素化するとともに、複数のアプリケーションで認証情報を共用可能とする情報処理装置を提供することにある。

【００１１】

【課題を解決するための手段】前記目的を達成する本発明は、ユーザが利用する際に認証を行う複数のアプリケーションの間で認証情報を共有可能とする認証システムであって、着脱自在な記憶媒体に記憶保持した記憶媒体が装着された状態にあり、且つ、認証済みである場合には、アプリケーション利用時に本人認証手順は行わず、そのままアプリケーションが実行され、一方、前記記憶媒体が外されている時は、アプリケーションを利用する際に本人認証を行うように切替制御する手段を備えたものである。

【００１２】

【発明の実施の形態】本発明の実施の形態について説明する。本発明は、コンピュータの利用者がコンピュータ上で動作するアプリケーションを利用する際に、アプリケーションによる利用者の本人認証を行うにあたり、本人認証を一度行えば、利用者が着脱自在な記憶デバイスをコンピュータから抜き取らない限り、すでに認証済み状態であれば、これ以降の本人認証を省略可能としたものであり、本人認証の操作・手続きを簡略化する。

【００１３】本発明の実施の形態について説明する。本発明の実施の形態は、図１を参照すると、認証要求手段（１）からの本人認証要求を認証情報検証手段（３３）が受け取り、本人認証情報の検証結果を認証結果通知手段（２）へ引き渡す。

【００１４】認証情報検証手段（３３）は、認証情報保持装置状態保持手段（３４）から認証情報保持装置の状態を取得し、活性化状態であれば、認証状態保持手段（３１）から認証状態情報（フラグ）を取得し、認証状態が未認証状態であれば、認証保持装置（４）が保持している本人認証情報と、認証検証手段（３３）が認証情報入力手段（３５）によって利用者から入力された認証情報との照合を行い、その結果を、認証結果通知手段（２）へ検証結果を供給する。

4

【００１５】認証情報検証手段（３３）は、認証状態保持手段（３１）から取得した認証状態が認証済み状態であれば、認証処理を省略し、認証結果通知手段（２）へ認証成功の旨を通知する。

【００１６】このようにして、認証状態を判断し、省略可能な認証手順を適宜省略することにより、認証手順を簡略化している。また一度、本人認証を行えば、他のアプリケーションでの本人認証手順を省略することができる。

【００１７】

【実施例】上記した本発明の実施の形態についてさらに詳細に説明すべく、本発明の実施例について図面を参照して説明する。図１は、本発明の一実施例の構成を示す図である。

【００１８】図１を参照すると本実施例は、アプリケーションが発行する認証関数（サブルーチン）群などの認証要求手段１と、認証結果を通知する認証結果通知手段２と、本人であるか否かの認証処理を行う認証手段３と、本人認証に必要となるパスワードや認証子（ＩＤ）などの本人認証情報を保持するフロッピーディスクや磁気カードなどの認証情報保持装置４と、を備えている。

【００１９】認証手段３は、利用者の認証が、未認証状態であるか認証済み状態であるかの情報を保持する認証状態保持手段３１と、認証情報保持装置４の特性等の情報を保持する認証情報保持装置情報保持手段３２と、利用者と認証情報保持装置４との認証インターフェースを制御する認証情報検証手段３３と、認証情報保持装置４が活性化されているか非活性化されているのかに関する状態情報を保持する認証情報保持装置状態保持手段３４と、利用者が保持する本人認証情報を入力するための認証情報入力手段３５とを含む。

【００２０】認証情報保持装置４は、認証情報を入出力するための認証情報入出力手段４１と、入力された本人認証情報を保持するための認証情報保持手段４２とを含む。

【００２１】これらの手段はそれぞれ概略つぎのように動作する。

【００２２】認証要求手段１は、情報処理装置で実行されるアプリケーションで利用者の認証が必要となった場合に該アプリケーションから起動され、本人認証を、認証情報検証手段３３に要求する。また、認証要求手段１が認証情報検証手段３３に対して要求した認証要求の結果は、認証情報検証手段３３から認証結果通知手段２に通知される。

【００２３】認証手段３の認証状態保持手段３１は、認証情報検証手段３３によって検証された結果を保持す

る。

【００２４】認証手段３の認証情報保持装置情報保持手段３２は、認証情報保持装置のハードウェア特性などの情報を保持する。

【００２５】認証手段３の認証情報検証手段３３は、認証情報保持装置状態保持手段３４から認証情報保持装置４の状態を取得し、活性化状態であれば認証状態保持手段３１から認証状態を取得し、当該認証状態が未認証状態であれば認証保持装置４が保持している認証情報と、認証検証手段３３が認証情報入力手段３５によって利用者から受け取った認証情報との検証を行い、その結果を、認証結果通知手段２へ検証結果を引き渡す。

【００２６】認証状態保持手段３１から取得した認証状態が認証済み状態であれば以降の処理を省略し、認証結果通知手段２へ検証結果（本人認証成功）を引き渡す。

【００２７】但し、認証情報保持装置状態保持手段３４から取得した状態が非活性化状態であれば、認証状態保持手段３１から取得した状態を無効とし、未認証状態の場合と同様の手順を取る。

【００２８】認証手段３の認証情報入力手段３５は、認証情報検証手段３３に要求された認証保持装置の特性に合った認証インターフェースのもと、利用者が入力した認証情報を認証情報検証手段３３へ供給する。

【００２９】認証手段３の認証情報保持装置状態保持手段３４は、認証情報保持装置４が活性化されているか非活性化状態にあるかの情報を保持する。

【００３０】認証情報保持装置４の認証情報入出力手段４１は、認証情報保持手段４２で保持されている認証情報の入出力を行う。

【００３１】図２、及び図３は、本発明の一実施例の動作を説明するためのフローチャートである。図１乃至図３を参照して本発明の一実施例の動作について説明する。

【００３２】まず、認証情報検証手段３３が認証要求手段１から要求された認証要求を受け付ける（図２のステップＡ１）。なお、認証要求手段１は、アプリケーションで本人認証を行うときに起動される。

【００３３】次に、認証情報保持装置状態保持手段３２から認証情報保持装置４の状態を受け取り（図２のステップＡ２）、使用する認証情報保持装置４が活性化状態か否かを判断する（図２のステップＡ３）。

【００３４】認証情報保持装置４が非活性化状態であれば、認証状態保持手段３１の認証状態を無条件に未認証状態とし、認証情報保持装置４の活性化を試みる（図２のステップＡ４）。

【００３５】認証情報保持装置４の活性化に失敗した場合、認証不可能と判断し、認証失敗を認証結果通知手段２に通知する（図２のステップＡ１２）。

【００３６】一方、活性化に成功した場合、認証情報保持装置状態保持手段３４の認証情報保持装置状態を活性化状態とし（図２のステップＡ５）、認証状態保持手段３１から認証状態を取得する（図２のステップＡ６）。

【００３７】図２のステップＡ３において、認証情報保持装置４が活性化状態であれば、図２のステップＡ４とステップ５をスキップし、図２のステップＡ６を実行する。

【００３８】取得した認証状態を検証し（図２のステップＡ７）、未認証状態であれば認証情報検証処理（図２のステップＡ８）を実行する。

【００３９】認証情報検証処理の結果を判断し（図２のステップＡ９）、検証失敗であれば図２のステップＡ１２を実行し、検証成功であれば、認証状態保持手段３１の認証状態を認証済み状態とし（図２のステップＡ１０）、認証成功を認証結果通知手段２に通知する（図２のステップＡ１１）。

【００４０】図２のステップＡ７で認証済み状態であれば、図２のステップＡ８とステップ９とステップ１０をスキップし、図２のステップＡ１１を実行する。

【００４１】次に、本人の認証情報の検証処理（図２のステップＡ８）を説明する。図３は、図２のステップＡ８の本人の認証情報の検証処理の処理手順を示すフローチャートである。

【００４２】まず、認証情報保持装置情報保持手段３２から装置情報を取得する（図３のステップＢ１）。

【００４３】本実施例では、認証情報保持装置４がフロッピーディスクや磁気カードなどの認証情報を保持する機能しか持たない装置であるため、認証情報保持装置４から認証情報を取得する（図３のステップＢ２）。この時、認証情報の取得に失敗したか否かを検証し（図３のステップＢ３）、失敗した場合、認証情報保持装置状態を非活性化状態とし、検証失敗とする（図３のステップＢ４）。

【００４４】ステップＢ３の判定で認証情報の取得に成功した場合、認証情報入力手段３５から利用者に対して利用者が保持している認証情報を入力させ（図３のステップＢ５）、図３のステップＢ２で取得した認証情報と、図３のステップＢ５で取得した認証情報を比較し、同じであれば検証成功とし、異なれば検証失敗とする（図３のステップＢ６）。

【００４５】次に、本発明の第２の実施例について説明する。図４は、本発明の第２の実施例の構成を示す図である、図４を参照すると、本発明の第２の実施例においては、図１に示した前記実施例と相違して、認証情報検証手段４３と認証情報入力手段４４が、認証情報保持装置４に含まれている。この認証情報保持装置４は、前記実施例で用いたフロッピーディスクや磁気カードなどのように情報を保持するだけではなく、例えばＩＣカード等のように、不揮発性の記憶手段のほかに制御装置（ＬＳＩ）を内蔵し、それ自身で認証情報の検証が可能とされ、また利用者からの認証情報を直接入力可能としてい

る。

【００４６】図５は、本発明の第２の実施例の処理を説明するための流れ図である。図を参照すると、図３に示したステップＢ１とからステップＢ２の間に、この実施例で用いられる認証情報保持装置４の特性によって、新たに２つのフェーズに分岐している。図５で追加された処理ステップについて以下に詳細に説明する。

【００４７】まず、認証情報保持装置情報保持手段３２から装置情報を取得し（図５のステップＢ１）、認証情報保持装置４自身に認証情報入力手段４４を保持しているか否かを判断する（図５のステップＣ１）。

【００４８】認証情報入力手段４４を保持している装置であれば、利用者に対して利用者が保持している認証情報を認証情報保持装置４に入力させ（図３のステップＣ３）、認証情報検証手段４３で検証した結果を認証情報検証手段３３が受け取る。この時、認証検証結果の取得に失敗した場合、認証情報保持装置状態を非活性化状態とし、検証失敗とする（図５のステップＣ５）。

【００４９】次に、認証情報保持装置４で認証情報入力手段４４を保持していなくとも、認証情報保持装置４が認証情報検証手段４３を保持していれば（図５のステップＣ２）、認証手段３の認証情報入力手段３５にて利用者から取得した（図５のステップＣ６）認証情報を、認証情報保持装置４へ入力し（図５のステップＣ７）、装置内の認証情報検証手段４３が、入力された認証情報と装置自身で保持している認証情報との検証を行う。

【００５０】検証結果を、認証情報検証手段３３が受け取る（図５のステップＣ８）。

【００５１】ステップ７で認証情報の入力に失敗した場合、認証情報保持装置状態を非活性化状態とし、検証失敗とする（図５のステップＣ５）。

【００５２】

【発明の効果】以上説明したように、本発明によれば、下記記載の効果を奏する。

【００５３】本発明の第１の効果は、最初に利用するアプリケーションで本人認証を行えば、その後、他のアプリケーションを利用する際に、本人認証を行う必要がなく、複数のアプリケーション間で認証情報を共有可能とし、利用者にとって使いやすいコンピュータ環境を提供することができる、ということである。

【００５４】その理由は、本発明においては、同じ認証情報保持装置を本人認証に用いるアプリケーション間では認証状態を共有することができるためである。

【００５５】本発明の第２の効果は、アプリケーションの設計において、汎用的な本人認証の機能を保持したアプリケーションを設計することを可能としている、ということである。

【００５６】その理由は、本発明においては、アプリケーション自体は、着脱自在の認証情報保持装置の特性を意識する必要がないために、認証情報保持装置の制御から解放される構成としたためである。

【図面の簡単な説明】

【図１】本発明の第１の実施例の構成を示す図である。

【図２】本発明の第１の実施例の処理を説明するための流れ図である。

【図３】本発明の第１の実施例の処理を説明するための流れ図である。

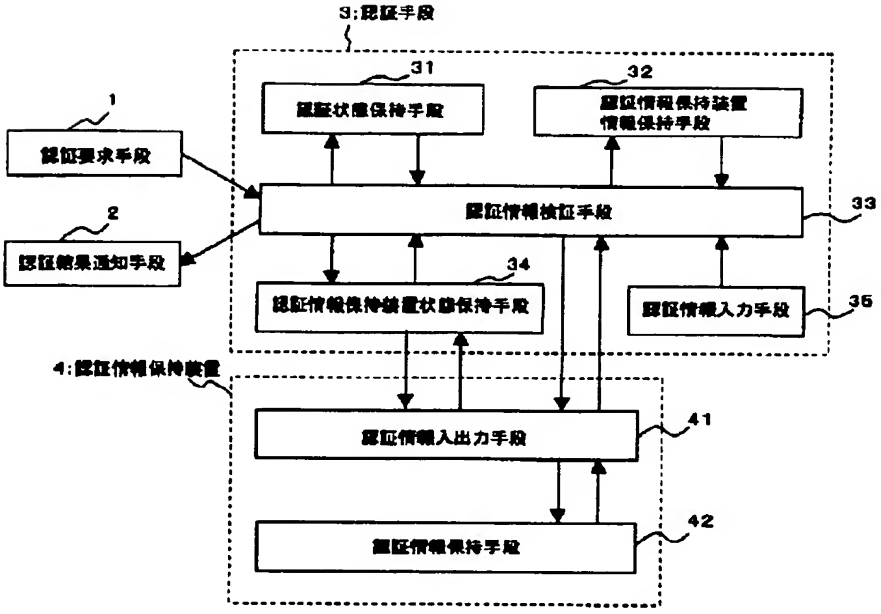
【図４】本発明の第２の実施例の構成を示す図である。

【図５】本発明の第２の実施例の処理を説明するための流れ図である。

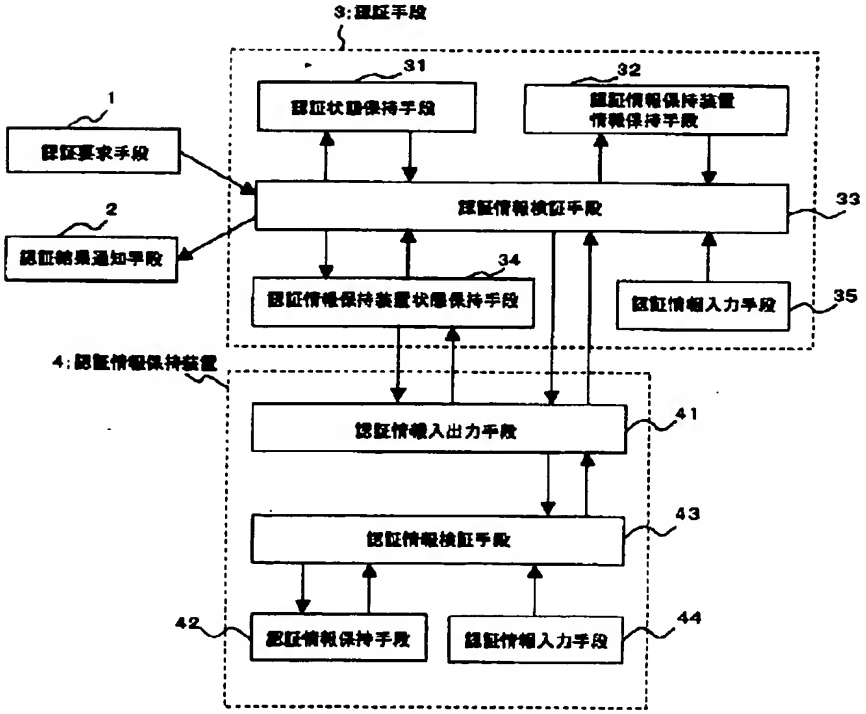
【符号の説明】

１　認証要求手段
２　認証結果通知手段
３　認証手段
４　認証情報保持装置
３１　認証状態保持手段
３２　認証情報保持装置情報保持手段
３３　認証情報検証手段
３４　認証情報保持装置状態保持手段
３５　認証情報入力手段
４１　認証情報入出力手段
４２　認証情報保持手段

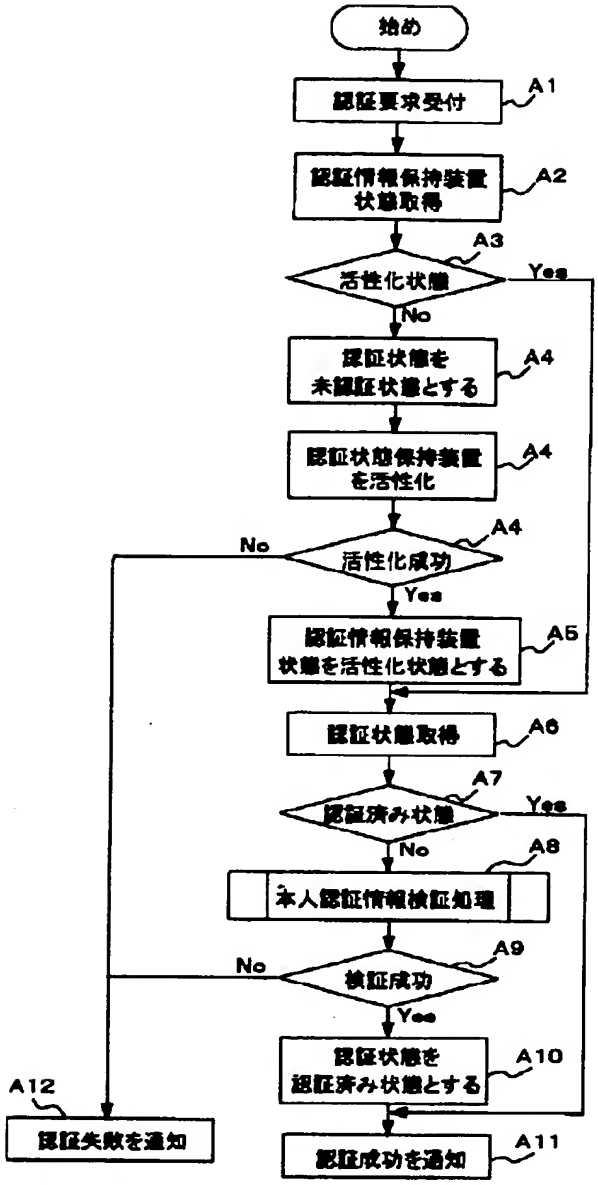
【図１】


3:認証手段
31
認証状態保持手段
32
認証情報保持装置
情報保持手段
1
認証要求手段
2
認証結果通知手段
認証情報検証手段
33
34
認証情報保持装置状態保持手段
認証情報入力手段
35
4:認証情報保持装置
認証情報入出力手段
41
認証情報保持手段
42

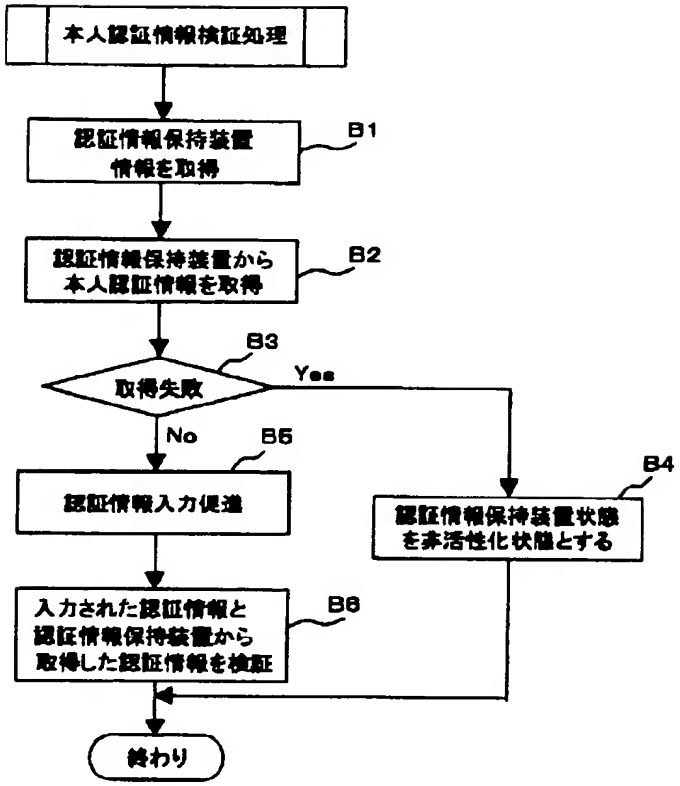
【図４】


3:認証手段
31
認証状態保持手段
32
認証情報保持装置
情報保持手段
1
認証要求手段
2
認証結果通知手段
認証情報検証手段
33
34
認証情報保持装置状態保持手段
認証情報入力手段
35
4:認証情報保持装置
認証情報入出力手段
41
43
認証情報検証手段
42
認証情報保持手段
44
認証情報入力手段

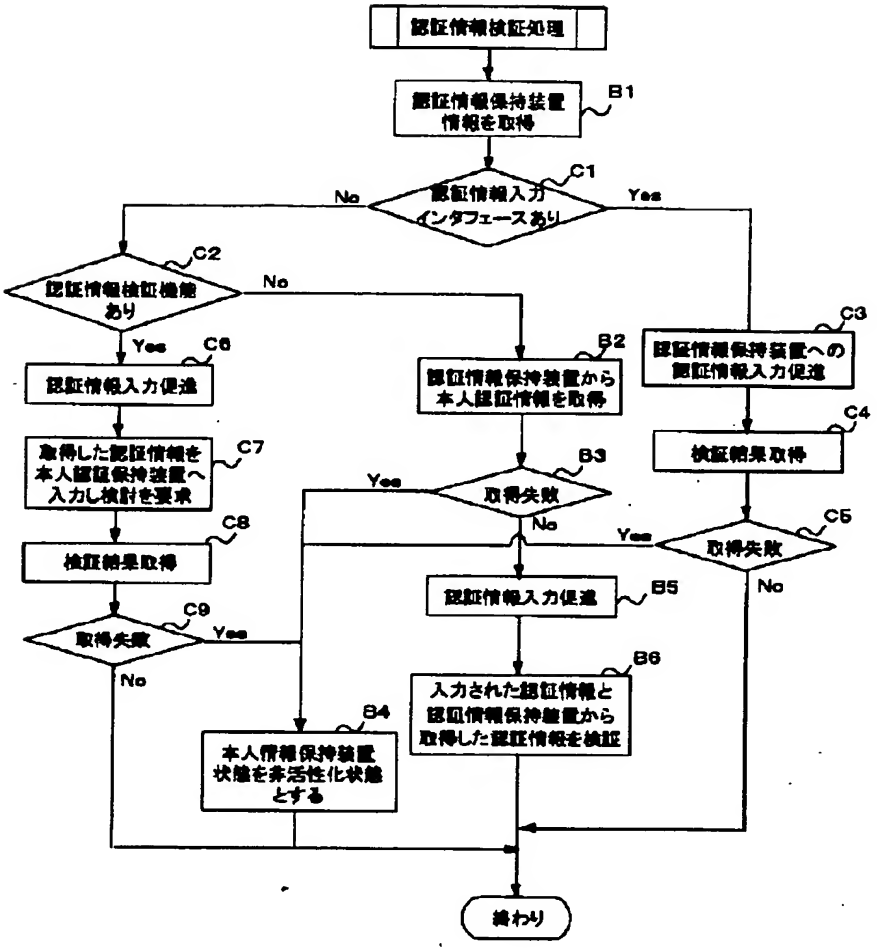
【図２】


始め
認証要求受付
A1
認証情報保持装置
状態取得
A2
A3
活性化状態
Yes
No
認証状態を
未認証状態とする
A4
認証状態保持装置
を活性化
A4
A4
No
活性化成功
Yes
認証情報保持装置
状態を活性化状態とする
A5
認証状態取得
A6
A7
認証済み状態
Yes
No
A8
本人認証情報検証処理
A9
No
検証成功
Yes
認証状態を
認証済み状態とする
A10
A12
認証失敗を通知
認証成功を通知
A11

【図３】


本人認証情報検証処理
認証情報保持装置
情報を取得
B1
認証情報保持装置から
本人認証情報を取得
B2
B3
取得失敗
Yes
No
B5
認証情報入力促進
B4
認証情報保持装置状態
を非活性化状態とする
入力された認証情報と
認証情報保持装置から
取得した認証情報を検証
B6
終わり

【図５】



フロントページの続き

(72)発明者　肥田野　守光
宮城県仙台市青葉区一番町１－10－23　東北日本電気ソフトウェア株式会社内

Ｆターム(参考)　5B085 AA08 AE06 AE12 AE23